SUBSTITUTE SPECIFICATION (Marked-up Copy)

PROCESS AND HIGHLY SECURE SYSTEM FOR THE DISTRIBUTION OF AUDIOVISUAL STREAMS

Related Application

[0001] This is a §371 of International Application No. PCT/FR2005/000636, with an international filing date of March 16, 2005 (WO 2005/101847 A1, published October 27, 2005), which is based on French Patent Application No. 04/50521, filed March 16, 2004.

Technical Field

[0002] ~~The present invention~~ This disclosure relates to the area of the highly secure distribution of digital audiovisual sequences.

~~[0003] The present invention proposes making available a process and a system that permit the visual and/or auditory protection of a digital audiovisual sequence issued from a digital compression standard or from a digital compression norm, the distribution in a highly secure manner of this sequence via a telecommunication network and the reconstitution of its original content from a protected audiovisual stream on a recomposition module of the equipment of the addressee.~~

~~State of the art~~

~~[0004] The US patent~~ US 6,351,538 ~~with the title "Conditional Access and Copy Protection Scheme for MPEG Encoded Video Data" is known from the state of the art.~~

[0005] ~~This document concerns the~~ discloses protection of a digital video stream. The protection is applied when the video stream is in the process of being digitized. The

digital video stream is considered as being composed of a stream of video images coded by compensation of movement and ~~of~~ a second stream of video image called a ~~reference~~ "reference" and serving to predict movement. ~~According to this document of the prior art~~ ~~the~~ The reference stream of video images is encrypted and the quantity of data to be encrypted ~~in order~~ to protect the stream is therefore reduced. The parameters that permitted this encryption operation to be realized are stored in the digital video stream in a part reserved for this purpose. The encryption of the reference images is sufficient to protect the content of the digital video stream because the rest of the digital video stream is composed of video image coded by compensation of movement from the reference video image stream. A double encryption operation is carried out, an encryption of the reference images by a first simple encryption function (application of an XOR or exclusive) then a complex encryption of the parameters of the first function by a second more complex encryption function. This double encryption allows the protection to be concentrated on the data quantity even less than the quantity that the reference images represent. The stream of video images coded by compensation of movement and the stream of reference video images (then protected) are then multiplexed ~~in order~~ to form the protected compressed video stream.

[0006] ~~This solution~~ That system does not provide a separation into two streams. It describes a decomposition into two sets composed ~~on the one hand~~ of reference video images and ~~of~~ video images obtained by compensation of movement ~~whereas our invention realizes a physical separation of the video stream into two streams, a modified main stream that is thus an auto-protected compressed video stream and a complementary stream~~.

~~[0007] The~~ Thus, the problem ~~of the present invention~~ is to preserve the format of the digital video stream and bring about the protection a posteriori ~~[Latin = inductively]~~ of the compression, which is not the case in ~~the invention of the document of the prior art~~

US '538 in which it is clearly stated that the protection is made during the encoding of the video stream.

[0008] Finally, no analysis of the original digital stream is preformed in order to analyze the conformity of the data in it. Consequently, ~~the invention of document D1~~ US '538 may render the protected digital video stream not in conformity with the standard from which it issued.

[0009] ~~The prior art also comprises the international patent~~ WO 03/007608 discloses ~~with the title "Motion Picture Encryption Method and Apparatus with Variable Security".~~

~~[0010] According to this document of the prior art the~~ protection of a digital video stream ~~is~~ realized by an encryption method at the level of variable security.

~~[0011]~~ The compressed video stream is divided into blocks with a fixed size. The protection is performed on these digital data blocks. The protection is performed on each block in turn. Only several bytes are encrypted in each block and the rest of the block remains unchanged. The choice of bytes to be protected is obtained by a pseudorandom generator or by a "look-up table". The byte selected can also be encrypted by using a "look-up table".

~~[0012] According to this document of the prior art only~~ Only three per cent of each block has to be encrypted ~~in order~~ to obtain a satisfactory degradation of the compressed digital stream rendering it illegible for a standard rendering apparatus.

[0013] ~~This solution of the prior art~~ That system does not perform a separation into two compressed video streams, ~~as our invention does~~ but performs its decomposition into blocks of a fixed size that are treated independently ~~in order~~ to encrypt some date of each block. The goal of ~~this~~ that encryption operation is to render the compressed video stream illegible for a standard decoder ~~and consequently the invention of document D2 is fundamentally different from our invention, that performs a protection operation while retaining the stream in conformity with the original format, that is, readable by a standard decoder~~.

[0014] It is currently possible to transmit audiovisual programs in digital form via broadcasting networks of the microwave, cable, satellite type, etc., or via telecommunication networks of the DSL (Digital Subscriber Line) or BLR (Loop Local Radio) type or via DAB networks (Digital Audio Broadcasting) as well as via any wireless telecommunication network of the GSM, GPRS, EDGE, UMTS, Bluetooth, WiFi type, etc. Moreover, to avoid pirating works broadcast in this manner, they are frequently encrypted or scrambled by various well-known means.

[0015] W. Zeng et al. published in the ACM Multimedia Proceedings of the International Conference in October, 1999 and titled "Efficient Frequency Domain Video Scrambling for Content Access Control" is also known for the area of encryption. That article describe a method of protecting digital data coding a multimedia content. The method is based on pseudorandom generators for generating three base pseudorandom operations (bit inversion, permutation and rotation of block of coefficients) that can be combined and controlled by encryption keys. The set of original data is present in the protected stream and access to the original content is entirely conditioned on possession or not of encryption keys. However, that solution does not use different modelings of pseudorandom generators nor data of the original stream such as a cryptographic key. Given that all the original data of the stream remains inside the protected stream, that method represents a classic encryption solution and, consequently, does not correspond to this disclosure.

[0016] Concerning the separation of an audiovisual stream into two parts in order to protect it, "Protecting VoD the Easier Way", Griwodz et al., Proceedings of the ACM Multimedia, September, 1998 describes a process of distribution via broadband networks or temporary servers and a point to point secure connection of protected multimedia content whose access is controlled and traced. The original auto visual stream is deliberately corrupted by a predetermined modification of certain bytes in the stream without any analysis of the structure and the content of the stream, therefore, without

taking account of the conformity with the native format, which bytes are selected according to a predefined law (Poisson's law). A signal permitting reconstruction is transmitted subsequently to the client at the moment of viewing the content: A key is first communicated to the client that allows the client to recalculate emplacement of the corrupted bytes in the stream. Then, a signal containing the original bytes is sent to the client after encryption to reconstruct the initial stream. Reconstruction of the stream is thus conditioned by a simple key and consequently does not provide a high level of security.

Summary

[0017] The disclosure, thus, relates to a process for distributing audiovisual sequences according to an original stream format having a succession of frames, the original stream on which an analysis is made, prior to transmission to client equipment, to generate a first modified main stream and complementary information, then the modified main stream and the complementary information are transmitted separately to equipment of an addressee, and for which a synthesis of a stream in the original format is calculated on the equipment of the addressee as a function of the modified main stream and the complementary information, wherein the analysis of the original stream includes:

an operation application stage comprising modelings generating sequences of pseudorandom values with known parameters,

a stage for the extraction of original data as a function of pseudorandom sequences, and

a stage for storage of the parameters of the modelings in the complementary information.

[0018] The disclosure also relates to a system for producing an audiovisual stream, including at least one multimedia server containing original audiovisual sequences, an

apparatus analysis of the audiovisual stream for separation of an original video stream into a modified main stream and into complementary information as a function of the analysis, at least one telecommunication network for transmission and at least one apparatus in the equipment of the addressee for reconstruction of the audiovisual stream as a function of the modified main stream and the complementary information.

[0019] The disclosure further relates to a process for distributing audiovisual sequences according to an original stream format having a succession of frames including:

performing modelings on the original stream to generate sequences of pseudorandom values with no parameters;

extracting original data as a function of pseudorandom sequences;

generating a first modified main stream and complementary information;

storing at least one parameter from the modelings in the complementary information;

separately transmitting the modified main stream and the complementary information to an addressee; and

synthesizing a stream in original format by equipment of the addressee as a function of the modified main stream and the complementary information.

Brief Description of the Drawings

[0020] Fig. 1 graphically shows a pseudorandom generator.

[0021] Fig. 2 schematically shows selected aspects of complementary information.

[0022] Fig. 3 schematically shows an example of a secure system for distributing audiovisual streams.

~~Subject matter of the invention~~ Detailed Description

[0023] The invention provides a process and a system that permit the visual and/or auditory protection of a digital audiovisual sequence issued from a digital compression standard or from a digital compression norm, the distribution in a highly secure manner of the sequence via a telecommunication network and reconstitution of its original content from a protected audiovisual stream on a recomposition module of the equipment of the addressee.

[0024] The ~~present~~ invention relates more particularly to an apparatus capable of transmitting in a secure manner via a telecommunication network a set of high-quality audiovisual streams to a viewing screen and/or ~~to~~ an audio output belonging to a terminal or to a display apparatus such as a television screen, a computer or even a mobile telephone, a mobile terminal of the PDA type (Personal Digital Assistant) or the like while preserving the audiovisual quality, but avoiding ~~any~~ fraudulent use such as the ~~possible~~ possibility of making pirated copies of the broadcast contents.

[0025] ~~The invention advantageously relates to~~ We disclose a process and a client-server system that protects the audiovisual contents by separating them into two parts, which second part is ~~absolutely~~ indispensable for ~~the~~ reconstitution of the original stream, ~~which~~ the latter of which is restored as a function of the combination of the first part.

[0026] The process ~~used in the present invention for the description of a preferred but non-limiting exemplary embodiment separates~~ may separate the audiovisual stream into two parts in such a manner that the first part called the "modified main stream" contains the quasi-totality of the initial information, e.g., more than 99%, and a second part called "complementary information" containing targeted elements of the original information and that is of a very small size relative to the first part.

~~[0027] It is currently possible to transmit audiovisual programs in digital form via broadcasting networks of the microwave, cable, satellite type, etc., or via~~

~~telecommunication networks of the DSL (Digital Subscriber Line) or BLR (Loop Local Radio) type or via DAB networks (Digital Audio Broadcasting) as well as via any wireless telecommunication network of the GSM, GPRS, EDGE, UMTS, Bluetooth, WiFi type, etc. Moreover, in order to avoid the pirating of works broadcast in this manner, they are frequently encrypted or scrambled by various well known means by the prior art.~~

~~[0028] The article written by W. Zeng et al. published in the ACM Multimedia Proceedings of the International Conference in October, 1999 and titled "Efficient Frequency Domain Video Scrambling for Content Access Control" is also known in the prior art for the area of encryption. In this That article the authors describe a method of protecting digital data coding a multimedia content. The method is based on pseudorandom generators for generating three base pseudorandom operations (bit inversion, permutation and rotation of block of coefficients) that can be combined and controlled by encryption keys. In this prior art the The set of original data is present in the protected stream and the access to the original content is entirely conditioned by the on possession or not of encryption keys. However, this that solution does not use different modelings of pseudorandom generators nor data of the original stream such as a cryptographic key. Given that all the original data of the stream remains inside the protected stream, this prior art that method represents a classic encryption solution and, consequently, does not correspond to the objectives of high security, subject matter of the present invention this disclosure.~~

~~[0029] Concerning the separation of an audiovisual stream into two parts in order to protect it, the prior art contains the article "Protecting VoD the Easier Way", Griwodz et al., Proceedings of the ACM Multimedia, September, 1998 in which the authors describe describes a process of distribution via broadband networks or temporary servers and a point to point secure connection of protected multimedia content whose access is controlled and traced. The original auto visual stream is deliberately corrupted by a~~

~~predetermined modification of certain bytes in the stream without any analysis of the structure and of the content of the stream, therefore, without taking account of the conformity with the native format, which bytes are selected according to a predefined law (Poisson's law). A signal permitting the reconstruction is transmitted subsequently to the client at the moment of the viewing of the content: A key is first communicated to the client that allows him the client to recalculate the emplacement of the corrupted bytes in the stream. Then, a signal containing the original bytes is sent to him the client after encryption in order to reconstruct the initial stream. The reconstruction Reconstruction of the stream is thus conditioned by a simple key and consequently the process described in this document of the prior art does not provide the a high level of security proposed in the present invention.~~

[0030] ~~The present invention~~ This disclosure also concerns modelings of pseudorandom processes used to define at which location and which modification will be applied, which modelings are a mathematical model describing a random natural phenomenon. These pseudorandom processes are initialized by different grains. The random process generating the grains is also modified dynamically by a set of parameters relative to its modeling during ~~the~~ generation of the pseudorandom sequence.

[0031] These initialization grains and ~~these~~ modeling parameters are advantageously the data extracted from the original stream. The protection applied to the contents distributed by the secure system ~~in the present invention~~ is advantageously based on the principle of ~~the~~ deletion and ~~the~~ replacement of certain information present in the encoded original audiovisual signal by any method such as: Substitution, modification, permutation or shifting of the information. This protection is also based on a knowledge of the structure of the digital stream. ~~The~~ This solution ~~consists in extracting~~ extracts and permanently ~~preserving~~ preserves in a secure server connected to the broadcasting and transmission network a part of the data of the audiovisual program recorded at the user's or directly broadcasted in this complementary information, which part is of prime

importance for reconstituting ~~this~~ the audiovisual program, but has a volume that is very small relative to the total volume of the digital audiovisual program recorded at the user's or received in real time by the user. The lacking part (the complementary information) will be transmitted via the secure network advantageously distributed by broadcasting or transmission at the moment of ~~the~~ viewing and/or ~~the~~ hearing of ~~this~~ the audiovisual program. The data removed in the original audiovisual program is advantageously substituted[,] ~~in order~~ to form the modified main stream[,] by random or calculated data called decoys.

[0032] The fact of having removed and substituted with decoys a part of the original data of the original audiovisual stream during ~~the~~ generation of the modified main stream does not permit ~~the~~ restitution of ~~this~~ the original stream only from the data of ~~this~~ the modified main stream. ~~In an embodiment this~~ The modified main stream ~~is~~ may be totally compatible with the format of the original stream and can therefore be copied and read by a reader, but it is completely incoherent from the viewpoint of human visual and auditory perception. ~~In another embodiment this~~ The modified main stream ~~has~~ may have any format.

[0033] Once the digital stream is separated into two parts, the largest part, the modified main stream, is then transmitted via a classic broadcasting network whereas the lacking part, ~~this~~ the complementary information, is sent on demand via a narrow band telecommunication network such as the classic telephone networks or cellular networks of the GSM, GPRS, EDGE or UMTS or by using a small part of a network of the DSL or BLR type, or by using a subset of the broadband shared on a cable network, or also via a physical support such as a memory card or any other support. In ~~a~~ particular, ~~embodiment~~ the two networks can be combined while retaining the two separate transmission paths. The audiovisual stream is reconstituted on the addressee's equipment by a synthesizing module from the modified main stream and ~~from~~ the complementary information sent piece by piece during ~~the using~~ use of the audiovisual stream.

[0034] The fact that the complementary information represents a quite small part of the original stream, e.g., 1%, allows it to be sent through networks with a low transmission rate. When the modified main stream has already been downloaded on the hard disk of the equipment of the addressee, the complementary information is preferably sent via a narrow band network. Complementary information with a low size facilitates its distribution on every type of network and contributes to ~~the~~ reinforcement of security.

[0035] The ~~subject matter of the present invention~~ disclosure further concerns an analysis module that implements a securing process in such a manner as to optimize the structure and ~~the~~ content of the complementary information with the aid of different algorithms and modelings ~~in order~~ to minimize the size of ~~this~~ the complementary information and to reinforce security.

[0036] The ~~present invention~~ disclosure also concerns ~~in its most general meaning~~ a process for ~~the distribution of~~ distributing audiovisual sequences according to an original stream format constituted ~~by~~ of a succession of frames, ~~this~~ the original stream on which an analysis is made, prior to ~~the~~ transmission to the client equipment, ~~in order~~ to generate a first modified main stream and complementary information, then the modified main stream and ~~the~~ complementary information are transmitted separately to the equipment of the addressee, and for which a synthesis of a stream in the original format is calculated on the equipment of the addressee as a function of ~~this~~ the modified main stream and ~~of this~~ the complementary information, which analysis of the original stream is constituted by:

[-]~~An~~ an operation application stage comprising modelings generating sequences of pseudorandom values with known parameters,

[-]~~A~~ a stage for ~~the~~ extraction of original data as a function of ~~these~~ the pseudorandom sequences, and

[-]~~A~~ a stage for the storage of ~~these~~ parameters of ~~these~~ the modelings in the complementary information.

[0037] ~~According to an embodiment these~~ The parameters ~~are~~ may be stored integrally in the complementary information.

~~[0038] According to another embodiment these~~ The parameters ~~are~~ may also be stored partially in the complementary information.

[0039] ~~These~~ The pseudorandom values advantageously represent information relative to at least one characteristic of the data extracted in the original stream.

~~[0040]~~ These pseudorandom values advantageously represent information relative to the position of the data extracted in the original stream.

~~[0041]~~ Furthermore, ~~these~~ the parameters of ~~these~~ the modelings are random.

[0042] ~~According to a variant these~~ The parameters of ~~these~~ the modelings ~~are~~ may be data extracted from the original stream.

~~[0043] According to another variant these~~ The modelings ~~are~~ may be random.

[0044] ~~These~~ The modelings are advantageously generated from at least one characteristic of the analysis equipment.

~~[0045] These~~ The modelings are advantageously stored in the analysis equipment.

~~[0046] In one embodiment these~~ The modelings used by the analysis equipment ~~are~~ may be sent in advance by the equipment of the addressee.

~~[0047] In another embodiment these~~ The modelings ~~are~~ may also be stored in a smart card of the equipment of the addressee.

[0048] ~~This synthesis~~ Synthesis of the original stream is preferably carried out as functions of the parameters of the modelings, reproducing the pseudorandom values obtained during the analysis stages.

[0049] Furthermore, the process is lossless.

[0050] ~~The present invention~~ We also ~~concerns~~ disclose a system for ~~the~~ implementation of the process, comprising at least one multimedia server containing the original audiovisual sequences, comprising an apparatus for ~~the~~ analysis of the audiovisual stream for ~~the~~ separation of the original video stream into a modified main

stream and ~~into~~ complementary information as a function of ~~this~~ the analysis, at least one telecommunication network for ~~the~~ transmission and at least one apparatus in the equipment of the addressee for ~~the~~ reconstruction of the audiovisual stream as a function of ~~this~~ the modified main stream and ~~of this~~ the complementary information.

~~[0051] The present invention will be better understood with the aid of the exemplary embodiments and of the detailed stages below.~~

[0052] The complementary information represents the set of data and information necessary for ~~the~~ reconstruction of the original stream. It advantageously contains the original extracted values, their positions and information necessary for ~~the~~ reconstruction, that are relative to the characteristics of ~~this~~ the original data of the stream. However, in this instance, the information about the position of the original data have a size on the order of 50% of the complementary information. ~~A compression~~ Compression of the complementary information proved to be ineffective on account of the fact that the positional information is statistically independent and therefore ~~with~~ has a low redundancy. Moreover, the presence of voluminous positional information limits ~~the~~ security all the more because there is so much original data that is not extracted, substituted by decoys and stored in the complementary information.

[0053] ~~The present invention advantageously proposes reducing~~ We reduce the ~~number~~ amount of information contained in the complementary information concerning the original data and ~~to~~ define it with the aid of modelings. In this manner, ~~this~~ the information is reproduced during ~~the~~ reconstitution of the original stream, the modelings and their parameters being known.

[0054] ~~A preferred but non-limiting exemplary embodiment~~ Representative, selected examples are described ~~in the present invention concerns~~ below with respect to modelings and algorithms of generators of pseudorandom sequences, initialized by random processes.

[0055] A random process is an, e.g., temporal signal s(t) for which the value can not be provided in advance whatever the considered instant. Such a process is generated either by using unforeseeable physical phenomena (such as the phenomena of the degradation of the atoms of radioactive elements) or by using pseudorandom processes coupled with random factors (such as an algorithm of the "wheel of fortune) type. Very complex (depending on phenomena not always mastered by ~~an expert~~ one skilled in the art) and with constraints on the execution time that are too great on a computer, random processes are generally used in combination with pseudorandom processes. Random processes are used for ~~the~~ modeling and initialization of pseudorandom generators.

[0056] A pseudorandom process is a deterministic process that allows ~~the~~ generation of a sequence of numbers that possesses a distribution selected in a more or less uniform manner. These processes are initialized by a grain that serves as a starting point for the sequence. The advantage of pseudorandom processes is that they are rapid (short execution time for a computer) because they are issued from not very complex mathematical calculations. The quality of a pseudorandom generator is measured as a function of its period (number of minimal values that the sequence contains before reproducing itself identically) and ~~of~~ the equidistribution that it will supply in several directions. An efficient pseudorandom generator has a long period and an equidistribution in a large number of direct actions.

[0057] An example of a pseudorandom generator of numbers (congruent linear pseudorandom generator) is described by the following expression, in which S_n is the term of the sequence, M-1 the maximal value for the term S_n, and A and B are respectively the slope and the ordinate at the origin of a straight line F of the equation:

$$S_{n+1}=(S_n*A+B) \bmod (M).$$

The term S_n represents in ~~our~~ this case the grain maintained as follows:

grain = (grain * 0x5DEECE66DL + 0xBL) &

((1L << 48) -1;

S_n=grain

A=0x5DEECE66DL

B=0xBL

mod (M) = & ((1L << 48) -1);

[0058] This pseudorandom generator has a theoretical period of 2^48, the operation & ((1L << 48) -1) ensures the periodicity by rejecting any value greater than 2^48. Multiplier A is selected in such a manner that an oscillation is rapidly obtained.

[0059] ~~Figure~~ Fig. 1 illustrates an example of a pseudorandom generator.

[0060] Successive values are generated from S_0 placed on the abscissa. The ordinate corresponding to the projection of S_0 on straight line F with slope A gives the value of the following grain S_1 on the ordinate, the value of which grain placed on the abscissa and projected from straight line F on the ordinate will give the value of the future grain S_2, and thus this iterative operation produces a sequence of grains.

[0061] When the grain is greater than or equal to the value S_{max}= (M-B)/A, the rest of the entire division (the "modulo" function) of the value generated for S_{max} divided by M is sent back to the generator to continue the sequence, result of the congruence of the modulo function.

[0062] ~~Exemplary embodiments~~ Representative, selected examples are described in the following that implement modelings of congruent linear functions that produce pseudorandom values that are used during the analysis and ~~the~~ synthesis.

[0063] The analysis performed ~~in order~~ to separate the original stream into a modified main stream and ~~into~~ complementary information advantageously uses a large number of

modelings of pseudorandom processes ~~in order~~ to guarantee a maximum of randomness and to thus furnish elevated security. This analysis is constituted ~~by~~ of the following stages:

[-]~~An~~ an operation application stage comprising modelings of pseudorandom processes, generating sequences of pseudorandom values with known parameters,

[-]~~A~~ a stage for ~~the~~ extraction of the original data as a function of ~~these~~ the pseudorandom sequences,

[-]~~A~~ a stage for ~~the~~ introduction of the decoy data in place of the extracted original data,

[-]~~A~~ a stage for ~~the~~ storage of ~~these~~ the parameters of ~~these~~ the modelings in the complementary information.

[0064] The protection process for each of the different digital formats has its own analysis algorithm constituted ~~by~~ of the enumerated stages in guaranteeing an audiovisual degradation. Including the pseudorandom processes, ~~this~~ the analysis ensures the unicity and ~~the~~ effectiveness of the protection. It is at this moment of the process that the degree of security introduced into a stream is defined from the possible combinations generated by the pseudorandom process. The pseudorandom sequences generated during the analysis are advantageously used for:

- Selecting the position of data to be extracted,
- Selecting the number of data to be extracted for a given stream portion,
- Selecting the size of the stream portion to be protected,
- Selecting the number of portions to be protected,
- Selecting the decoys and inserting them in place of the original data.

[0065] As concerns the evaluation of the degree of security introduced, the known AES ("Asymmetric Encryption System") protection process by encryption is taken as reference from the prior art. The key has a length of 128 bits and the number of possible combinations is therefore:

2^{128}=3.40e+8 possibilities of a key with 128 bits.

[0066] ~~The~~ We pose the hypothesis ~~is posed in the present invention~~ that all the events are random, a stream portion with a length of 300 bytes is taken in which "n" = 5 decoys, for example, is added, each of which decoys has a length of one byte. The following result is obtained: An account is taken of all the combinations of 5 bytes among 300, which makes 1,96e+12 possible words, knowing that there are 2^{40} binary words or 1,10e+12 possible words, and a total of 2.37e+34 possibilities are finally obtained. It was assumed that the number of decoys for realizing this calculation was known, namely, 5 decoys for a portion of 300 bytes. In the case in which the value of "n" would not be known, the total number of possibilities is obtained by summing the results for each of the "n" from 1 to 300, which produces a considerably augmented number of possibilities. [-]~~with~~ With 300 decoys there is a combination of 300 bytes among 300 and 2^{2400} possible binary words, therefore, plus n (the number of decoys) is great the more the number of possibilities increases. However, the preceding hypothesis considers that all the samplings are random except in a real case of an analysis algorithm the sequences generated are pseudorandom, therefore, an ill-intentioned person could decide to search for the grain from which the pseudorandom sequence was generated. Knowing that the positions were generated by a grain of 32 bits over an interval of 300 values, this yields $2^{32}*256^{5}$=4.73e+21 possibilities for finding the values of the positions of the decoys (for a grain of 64 bits, 2.10e+31 possibilities are obtained, and likewise it is necessary to make the sum from 1 to 300 for each possible “n” in the portion described). In conclusion, it is easier for an ill-intentioned person to search for the grain than an exhaustive search of the positions of the decoys from the protected stream. However, when a grain coded for 128 bits is selected, the number of possibilities for the grain is identical to the number of keys possible for the AES method with a key coded for 128 bits.

[0067] Since an algorithm can not be composed solely of random processes as concerns rapidity of execution, the use of a pseudorandom generator becomes necessary for which generator a random grain is used that permits the desired security level to be fixed, e.g., by selecting a grain with a length of 128 bits. Likewise, a judicious choice of the parameters A, B, M and S_0 is carried out in such a manner as to generate pseudorandom sequences with different types of distribution.

[0068] In this instance, a criterion for the evaluation of the security is the number of grains necessary for the process and the manner in which the sequences are generated.

[0069] The parameters A, B, M and S_0 for ~~the~~ modeling ~~of~~ the generator are advantageously selected randomly and remain unchanged for a portion of a given stream, e.g., for N consecutive bytes. At the end of this portion the parameters A, B, M and S_0 are modified, thus, reselected in a random manner. In this manner, the set of modeling parameters A, B, M and S_0 is changed every N bytes and N itself is advantageously random. The set of modeling parameters A, B, M and S_0 is preferably changed each time that the value S_{max} is exceeded.

[0070] As concerns ~~the~~ recomposition of the original stream during the synthesis on the equipment of the addressee, it is indispensable to recover the original values of the data extracted from the original stream and their placements in the stream. However, storing their true values and their placements in the complementary information produces ~~a~~ complementary information containing much data that can be recalculated from the modeling parameters used during the analysis. Consequently, ~~an~~ optimization of the size of the complementary information is performed by storing in the interior only the original extracted data and modeling parameters from which the positions and other characteristics of the original data are reproduced during the synthesis on the equipment of the addressee. Consequently, since the data relative to the original positions is on the order of 50% of the complementary information, the size of the complementary information is greatly reduced, all the while ensuring ~~the~~ audiovisual degradation and

increasing ~~the~~ security because it furnishes the possibility of extracting more original data and of introducing more decoys.

[0071] ~~In another embodiment the~~ The original data ~~is~~ may be extracted without ~~the~~ introduction of decoys in its place.

[0072] The analysis determining the characteristics of the data to be extracted is carried out taking three constraints into account:

- The degradation of the content,
- The security,
- The transmission rate of the complementary information.

Since the relationship between these three constraints is very complex, it is proposed to reduce the size of the complementary information without, however, reducing ~~the~~ security and ~~the~~ audiovisual degradation.

[0073] ~~Figure~~ Fig. 2 represents the complementary information containing ~~the~~ values generated by the modeling, namely, the positions P (~~figure~~ Fig. 2a) and the original extracted data D. Figure ~~2d~~ 2b represents the complementary information containing the modeling parameters S and the original extracted data D.

[0074] The complementary information preferably contains original data D. The modeling parameters or grains S from which these positions are generated are backed up in the place of positions P. The grains are advantageously ~~the~~ data extracted from the original stream, thus guaranteeing high randomness or a combination of ~~this~~ the data, which brings about an increase ~~of~~ in the complexity of the ~~chaining~~ chain between grains. For example, a grain is selected for the first position using a random process and a second grain combination of the first grain with the value of the extracted data is made for the second position of data to be extracted, and so forth. This operation guarantees for each random process a random re-initialization of the generator (the extracted value being random). ~~In order to avoid a portion of the protected stream from being compromised in the case that the first grain would be found, a~~ A grain of 64 bits or 128

bits generated by a true random process is selected to avoid a portion of the protected stream from being compromised in the case that the first grain would be found. It proved to be difficult in this case to reconstitute the original positions since the positions are modeled from the grain in combination with the values of the original data of the stream.

[0075] The original content of the stream is restored from value S of the grain or the parameters or the model and the original data contained in the complementary information by the synthesis module that will reconstruct the original stream on the equipment of the addressee.

[0076] The complementary information is preferably specific to the analysis equipment that generates it with the aid of characteristics belonging to ~~this~~ the equipment. Consequently, the complementary information will be freely broadcast because it can be interpreted solely by ~~this~~ the analysis equipment or by other analysis equipment having exactly the same characteristics. The pseudorandom generator advantageously has a modeling belonging to the analysis equipment and/or relative to at least one characteristic belonging to the analysis equipment. ~~In one embodiment these~~ The modeling ~~are~~ may be stored in the analysis equipment. ~~In another embodiment these~~ The modelings ~~are~~ may also be stored in the equipment of the addressee. ~~These~~ The modelings are advantageously stored in a smart card of the equipment of the addressee. ~~These~~ The modelings of the equipment of the addressee are preferably sent to the analysis equipment for ~~the~~ generation of complementary information personalized for the equipment of the addressee.

[0077] ~~Figure~~ Fig. 3 shows a scheme with a purely explanatory description of a preferred a ~~non-limiting embodiment particular to~~ a client-server system for implementing the process ~~in accordance with the invention~~.

[0078] Original audiovisual digital stream 1 to be secured is passed via a link 2 to analysis and protection module 31 that generates modified main stream 32 in a format advantageously identical to the format of input stream 1, aside from which certain

original data was replaced by values different from the original ones and stored on server 3. The complementary information 33 in any format contains the values of the original data and the modeling parameters relative to the characteristics of the original modified, replaced, substituted or moved data. ~~This~~ The complementary information 33 is also stored on server 3.

[0079] Modified main stream 32 is then transmitted via high-throughput network 5 of the microwave, cable, satellite type, etc., to the terminal of user 8 and ~~is~~ stored in memory 81, that can be, e.g., a hard disk. When user 8 requests to view the audiovisual sequence present in ~~his~~ memory 81, two things are possible: In the first instance, user 8 does not have all the rights necessary to view the audiovisual stream and in this instance audiovisual stream 32 generated by analysis module 31 present in ~~his~~ memory 81 is passed to synthesis system 86 via reading buffer memory 83 that does not modify it and transmits it identically to a reader capable of decoding it 87, and its content, degraded visually and/or auditorily by scrambling module 31 is displayed on viewing screen 9.

[0080] In the second instance, server 3 decides that user 8 has the rights to view the audiovisual stream. In this instance, synthesis module 86 makes a viewing request to server 3 containing complementary information 33 necessary for ~~the~~ recomposition of original sequence 1. Server 3 then sends complementary information 33 via telecommunication networks of the analog or digital telephone line type, DSL (Digital Subscriber Line) or BLR (Loop Local Radio) type, via DAB networks (Digital Audio Broadcasting) or via digital mobile telecommunication networks (GSM, GPRS, UMTS) 7, which permits ~~the~~ reconstitution of the original audiovisual stream in such a manner that user 8 can store it in buffer memory 85. Network 7 can advantageously be of the same type as network 5.

[0081] Network 7 can advantageously be combined with network 5.

[0082] Synthesis module 86 then proceeds to the recomposition of the original audiovisual stream from the modified main stream that it reads in its reading buffer

memory 83 and from the complementary information read in buffer memory 85 that permits it to recognize the positions as well as the original values of the modified data. The audiovisual stream reconstituted in the original format is sent to reader-decoder 87 corresponding to this format. The original reconstituted audiovisual stream is then displayed on viewing screen 9 of user 8.

[0083] Modified main stream 32 is advantageously passed directly via network 5 to reading buffer memory 83 then to synthesis module 86.

[0084] Modified main stream 32 is advantageously inscribed (recorded) on a physical support like a disk of the CD-ROM or DVD type, a hard disk or a memory card 4. Modified main stream 32 is then read from physical support 4 by reader 82 of box 8 ~~in order~~ to be transmitted to reading buffer memory 83, then to synthesis module 86.

[0085] Complementary information 33 is advantageously recorded on a physical support 6 with a credit card format constituted ~~by~~ of a smart card or a flash memory card. This card 6 is then read by card reader 84 of the apparatus of user 8.

[0086] Card 6 advantageously contains the algorithms and the modelings of the generator of pseudorandom sequences that will be executed by synthesis system 86.

[0100] Apparatus 8 is advantageously an autonomous, portable and mobile system.

ABSTRACT

A process for ~~the distribution~~ distributing ~~of~~ audiovisual sequences according to an original stream format ~~constituted by~~ having a succession of frames, ~~this~~ the original stream on which an analysis is made, prior to ~~the~~ transmission to ~~the~~ client equipment, ~~in order~~ to generate a first modified main stream and complementary information, then the modified main stream and the complementary information are transmitted separately to ~~the~~ equipment of ~~the~~ our addressee, and for which a synthesis of a stream in the original format is calculated on the equipment of the addressee as a function of ~~this~~ the modified main stream and ~~of this~~ the complementary information, ~~characterized in that this~~ wherein the analysis of the original stream ~~is constituted by~~ comprises:

[-]~~An~~ an operation application stage comprising modelings generating sequences of pseudorandom values with known parameters,

[-]~~A~~ a stage for the extraction of ~~the~~ original data as a function of ~~these~~ pseudorandom sequences, and

[-]~~A~~ a stage for ~~the~~ storage of ~~these~~ parameters of ~~these~~ modelings in the complementary information.